REMARKS

The October 17, 2006 Office Action regarding the above-identified application has been carefully considered; and the claim amendments above together with the remarks that follow are presented in a bona fide effort to respond thereto and address all issues raised in that Action. Care has been taken to avoid entry of new matter. For reasons discussed below, it is believed that this case is in condition for allowance. Prompt favorable reconsideration of this amended application is requested.

Definiteness of the Pending Claims

The Office Action included a rejection of claims 47-61 under the second paragraph of 35 U.S.C. § 112, essentially on the ground that various uses of the word "if" rendered the claims indefinite. By amendment above, Applicants have deleted each instance of the word "if" from the claims. As such, it is believed that the amended claims positively recite the appropriate determinations and/or responsive operations or functions, in a clear and concise manner. Applicants respectfully submit that the amended claims are definite and request withdrawal of the rejection under the second paragraph of 35 U.S.C. § 112.

Novelty Over the '878 Document

The Office Action included a rejection of claims 47-61 under 35 U.S.C. § 102(e) for anticipation over US patent application publication number 2004/0225878 to Costa-Requena et al. (hereinafter the '878 document). It is respectfully submitted that the anticipation rejection based on the '878 document is improper and should be withdrawn, and that the pending claims recite limitations that are absent from the technology actually disclosed by the '878 document.

Anticipation requires disclosure in a single prior art reference of each element of the claim under consideration. There must be no difference between the claimed invention and the

reference disclosure, as viewed by a person of ordinary skill in the field of the invention. In rejecting claims, the burden always is on the Patent Office and thus the Examiner to show all elements of a prima facie case barring Applicants' claims; and in the case of an anticipation rejection, this means that the Examiner is required to provide evidence and/or a cogent explanation of how the one applied prior art reference actually discloses each element of Applicants' claims either literally or on a theory of inherency. The rejection based on the '878 document does not provide an explanation or evidence of how the '878 disclosure actually meets applicants' claims, and for reasons discussed in the prior response, it is believed that the '878 document does not in fact disclose either the method of claim 47 or the system of claim 57.

The rejection parrots Applicants' claims and cites repeatedly to paragraphs 0031-0036, 0048-0050, 0068 and 0078-0079 of the '878 document, to allegedly satisfy virtually every recitation of Applicants' claims, **without any explanation whatsoever as to how the technology in the cited '878 texts corresponds to Applicants' claims**. For example, the independent claims both refer to "a control node" of the wireless communication network and a "server" for a data application. Claim 57 also refers to an authentication and authorization server, and both independent claims recite functions disclosed by Applicants as involving interactions of the an authentication and authorization server with the node to enable a user to access the data application running on the application server. The rejection does not identify the control node, the application server or the authentication and authorization server. As a result, the various cited sections of the text pointedly fail to explain or show how the '878 document allegedly satisfy virtually every recitation of Applicants' claims. Applicants have previously explained their interpretation of the '878 document and why that document does not satisfy Applicants' claims; and the mere citation of a multitude of text paragraphs without explanation is

not enough to refute Applicants' interpretation. In fact, the rejection does not make clear how the Examiner is applying the '878 document, and at least for that reason, the rejection over the '878 document is improper and should be withdrawn.

In addition, Applicants respectfully submit that a proper comparison of the actual disclosure of the '878 document to Applicants' claims leads to the conclusion that the document does not in fact meet all of the requirements of Applicants' claims. A detailed discussion of the distinctions of the claims over the actual disclosure of the '878 document follows.

Applicants' claim 47 relates to a method for managing authentication and authorization of user access to data applications of a service provider through a wireless communication network. The recited method involves authenticating a mobile station of a data application user as a valid mobile station for obtaining communication service through the wireless communication network, **at a control node of the wireless communication network**. In Applicants' disclosed arrangement, this node is a home location register or "HLR." The claim also recites obtaining information indicating successful authentication of the user's mobile station, from the control node. An identifier associated with the data application user is received, when the user attempts to access a data application on a server through the wireless communication network. Two types of determinations are made, one for station authentication, and one for user authorization relative to the particular application. Based on the identifier, there is a check of the information (i.e. of the information obtained from the network control node) to determine whether or not there has been a successful authentication of the user's mobile station at the control node. In response to a determination that there has been a successful authentication of the user's mobile station at the control node, the identifier is used to determine whether or not the user is authorized to access the data application on the server, from among a

number of data applications accessible through the wireless communication network. In response to a determination that the user is authorized to access the data application on the server, the method involves allowing the user to access the data application on the server from the mobile station via communications through the wireless communication network. Stated another way, access to the particular data application is allowed when the mobile station has been successfully authenticated by the network control node AND the user is authorized for access to the particular application among the number (plural) that are available.

Applicants' claim 57 relates to a system comprising a wireless network, a control node for authenticating one of the mobile stations of a data application user as a valid mobile station for obtaining communication service through the wireless network, a data application server, and an authentication and authorization server. The authentication and authorization server is configured for obtaining from the control node information indicating successful authentication of the data application user's mobile station. The authentication and authorization server receives an identifier associated with the data application user from the data application server, when the user attempts to access the data application service on the data application server through the wireless communication network. Based on the identifier, the authentication and authorization server checks the information (from the network control node) to determine whether or not there has been a successful authentication of the user's mobile station at the control node of the wireless communication network. In response to determination that there has been a successful authentication of the user's mobile station at the control node, the authentication and authorization server uses the identifier to determine whether or not the user is authorized to access the data application on the server, from among a plurality of data applications accessible through the wireless communication network. In response to a

determination that the user is authorized to access the data application on the server, the authentication and authorization server enables the data application server to permit the user to access the data application service from the mobile station via communications through the wireless communication network.

It is respectfully submitted that the technology actually disclosed by the '878 document does not in fact perform authentication and authorization functions corresponding to those recited in Applicants' independent claims.

It is Applicants' position that the '878 document actually discloses a technique facilitating generic authentication within an IP network, which uses a plurality of network elements that employ different authentication protocols and a central authentication server 134 arranged to provide authentication service in response to received authentication requests from the various network elements (paragraph [0011]). For example, if authentication is requested from a WLAN access point, such as the RAS 142, the authentication server 134 receives information about the algorithm and protocol and will return the security tokens formatted into the indicated protocol for that particular network element, such as the Extensible Authentication Protocol (EAP). Attention is directed to paragraph [0034]. Similarly, for SIP call authentication the authorization server 134 calculates necessary security keys or credentials ([0035]) and provides the necessary information to the CSCF 110 to perform the actual authentication ([0036]).

The technique disclosed in the '878 document purportedly supports a 'single single sign-on' service in which, if a user has already authenticated himself with one service provider, the user need not authenticate himself with a second service provider. In the disclosed method, the

sign-on at the first service provider lends itself to the second service provider, thus allowing the disclosed type of single sign-on. Attention is directed to paragraph [0050].

It is respectfully submitted that the '878 document does not suggest reliance on network validation of the user's mobile station as a user authentication for accessing a data application, in the manner recited in the independent claims now pending in this case. In the '878 publication, an element requiring authentication implements the actual user authentication based on its own protocol, albeit using information supplied from the central authentication server. For example, if authentication is requested from a RAS 142 or CSCF 110, the authentication server 134 receives information about the particular algorithm and protocol and returns the appropriate security data to facilitate authentication through the requesting device. Attention again is directed to paragraph [0034] - [0036]. In such an arrangement, there is no use of an identifier associated with the data application user to check if there has already been a successful authentication of the user's mobile station at a control node of the wireless communication network and attendant further processing if such prior authentication has occurred.

As noted, the '878 publication does mention support for a 'single sign-on' in which a sign-on at a first service provider lends itself to a second service provider (paragraph [0050]). However, the limited disclosure on the point appears only to teach use of an additional 'liberty manager 324' to separate the message schemas from their associated profiles and bindings. It is respectfully submitted that this addition to the authentication server 434 disclosed in the '878 publication would not suggest to one of skill in the art a technique in which an identifier associated with the data application user is used to check if there has already been a successful authentication of the user's mobile station at control node of the wireless communication network and attendant further processing if such prior authentication has occurred.

It is further submitted that the '878 publication does not fairly suggest the recited authorization related steps or functions. In the '878 publication, when the authentication service is operating on the network side, the authentication server provides the authentication service to a network element that is being accessed by a client, who must first be authenticated. In that case, the network element receives the attempt to access the network from a user supplying his own security credentials, and then forwards the credentials to the authentication server for validation. The authentication server will insure that the security credentials provided are correct according to the specific authentication protocol selected for the process (paragraph [0070]). However, it is not seen that the processing will further check user authorization to access the particular service, e.g. offered through the particular network element that received the attempt to access the network from the user. As such, the '878 publication does not satisfy the claim requirement for (after there has been a successful authentication of the user's mobile station at the control node of the wireless communication network) using the identifier to determine if the user is authorized to access the one particular data application on the server, from among a plurality of data applications accessible through the wireless communication network, and if so allowing the user to access that data application on the server from the mobile station.

In view of the above-noted claim requirements not met by the '878 publication, it is believed that independent claim 47 and independent claim 57 are both novel over that publication. The other pending claims depend from either claim 47 or claim 57 and should be novel for at least the same reasons. Withdrawal of the rejection over the '878 document is respectfully requested.

Novelty Over the Forslow Document

Claims 47-61 also stand rejected under 35 U.S.C. § 102(e) as anticipated by US patent application publication number 2003/0039237 to Forslow (inaccurately cited at several points as Bass et al.). This rejection is traversed.

Forslow discloses a gateway node that provides a common access server. The common access permits a mobile station that has initially established a communications session with an external network entity to perform only a single, common access procedure for subsequent communications using one of the circuit-switched and packet-switched networks. After that common access procedure is completed, subsequent application flows between the mobile station and the external network entity are established using abbreviated procedures without having to access the external network entity. Attention is directed to the last ten lines of the Abstract, to FIG. 11 and to the discussion in paragraphs 0093-0102.

The rejection concludes that the above-discussed disclosure by Forslow satisfies the claim requirements. Applicants disagree. It is not seen how Forslow relies on the wireless network authentication to support application layer authentication. It appears that the gateway provides a second authentication function after session establishment through the wireless network. Also, it is not apparent where Forslow teaches the subsequent authorization determination with respect to the particular application that the mobile station user is attempting to access from among some plurality of applications accessible through the wireless network.

Hence, it is believed that Forslow does not meet the pending claim requirements. For example, it is believed that Forslow does not disclose checking the information obtained from a network control node to determine whether or not there has been a successful authentication of the user's mobile station at the control node, or any determination of whether or not the user of

the authentic mobile station is also authorized to access one data application on the server from among a number of data applications accessible through the network, in response to the determination that there has been a successful authentication of the user's mobile station at the control node, as required by the independent claims.

Forslow therefore does not meet all recitations of either of the independent claims, and the rejection over Forslow is improper and should be withdrawn.

Novelty Over the Pirila Document

Claims 47 and 57 also stand rejected under 35 U.S.C. § 102(e) as anticipated by US patent application publication number 2003/0152232 to Pirila et al. (hereinafter Pirila). This rejection is traversed.

Pirila discloses a technique for managing unencrypted communications for a mobile station. The subscriber data in a home network (HLR) of a subscriber (UE) is provided with a subscriber ciphering profile which indicates whether an unciphered call, session or data packet is to be rejected, accepted or handled in some other manner. A serving network (MSC/VLR, SGSN, UTRAN) checks the subscriber ciphering profile and rejects or accepts the unciphered call, connection, session, or data packet, respectively, according to the subscriber ciphering profile.

The rejection concludes that the above-discussed disclosure by Pirila satisfies the requirements of claims 47 and 57. Applicants disagree. To the contrary, Pirila deals only with the session through the wireless network(s). It is not seen where Pirila teaches authentication or authorization vis-à-vis an application server via a session, after authentication by the wireless network domain. Hence, it is believed that Pirila does not meet the pending claim requirements regarding network control node authentication of the mobile station, checking for that

authentication upon an attempt to access an application, and if authenticated, checking authorization for the specific server application. For example, it is believed that Pirila does not disclose checking the information obtained from a network control node to determine whether or not there has already been a successful authentication of the user's mobile station at the control node, or any determination of whether or not the user of the authentic mobile station is authorized to access one data application on the server from among a number of servers accessible through the network, in response to the determination that there has been a successful authentication of the user's mobile station at the control node, as required by the independent claims.

Hence, Pirila does not meet all recitations of either of the rejected claims, and the rejection of claims 47 and 57 over Pirila is improper and should be withdrawn.

Conclusions

Claims 47-61 remain active in this application. In view of the claim amendments presented herein, all of the pending claims should now be reasonably clear, concise and definite. For reasons discussed in detail above, Applicants submit that all of the pending claims distinguish over the art applied in the latest Office Action. Hence, all rejections should be withdrawn, and all of the claims should be in condition for allowance. Applicants therefore respectfully request prompt favorable reconsideration of their amended application.

It is believed that this response addresses all issues raised in the October 17, 2006 Office Action. However, if any further issue should arise that may be addressed in an interview or by an Examiner's amendment, it is requested that the Examiner telephone Applicants' representative at the number shown below.

To the extent necessary, if any, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8603 KEG:apr
Facsimile: 202.756.8087
Date: January 16, 2007

Please recognize our Customer No. 20277 as our correspondence address.